REMARKS

Applicant respectfully submits that the present invention as claimed does not contain new matter and is not anticipated by or obvious over the cited references. All claims are now present for examination and favorable reconsideration is respectfully requested in view of the following comments.

REJECTIONS UNDER 35 U.S.C. § 112 FIRST PARAPGRAPH:

Claims 1 – 4 have been rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to satisfy the written description requirement and containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Applicant respectfully submits that replacing the term "dual-locus operation" by the term "two-place operation" is not adding new matter. In the original specification, different types of operations performed on two operands (a data subblock and a subkey) are generalized with the term "two-place operation", which was translated into the English language with the term "dual-locus operation". "Dual-locus operation" is an alternative version of English translation of the Russian language term "two-place operation" which also exists in English. The translator of the specification chose "dual-locus operation" instead of "two-place operation". Applicant respectfully submits that the term "two-place operation" and the term "two-place operation" refer to the same subject matter. The Russian language original specification contains the term "two-place operation", which demonstrates that by the moment of the filing of the application for invention, the inventors possessed the claimed invention.

Furthermore, examples provided in the original specification (both in Russian and in English) indicate the use of operation of summation performed on a subblock and converted subkey. Operation of summation is commonly known to be a "two-place operation." Thus, in the original specification, two-place operation is used and this is

it to the operation unit (block, arrangement) 420 (processing means 420), which converts the digital input block M. In total, the cryptographic device described by Den Boer in Fig.4 and lines 35-65, column 4, contains three input units for receiving digital data: (1) "first input means 410" (line 40, column 4), i.e. unit 410 on Fig.4 means an arrangement for receiving an input data block and it is designated in Fig.4 as IM-1 (IM is an abbreviation of "input means"); (2) "second input block 440" (line 68) serving to receive key K1 and designated in Fig.4 as IM-2 (IM is abbreviation of "input means"); and (3) "third input block 450" (line 58) serving to receive key K2 and designated in Fig.4 as IM-3 (IM is abbreviation of "input means"). The term "third input block 450" means a device for receiving the key and **not data blocks** to be converted, as evidenced also by the fact that Den Boer calls data blocks "digital input blocks" (lines 40-41, 45, 47, 48, 50, 51, 53, 59, 60), "digital output block" (in lines 46, 47, 49, 51, 55, 63), "data block" (line 53).

Therefore, confusing used of terminology by Den Boer lies in the fact that two different terms "means" and "block" are used in referring to the units of the cryptographic device, which has misled the Examiner in understanding the essence of the invention of Den Boer. Therefore, the Examiner has unjustifiably broadened interpretation the disclosure of Den Boer.

As previously pointed out, in Den Boer, round subkeys are generated according to a determined law. Therefore, during the encryption of various data blocks, the value of subkeys remains unchanged over a preset conversion step of some preset round in the encryption methods described in Den Boer. More specifically, the description at col. 5, lines 44 – 55 of Den Boer shows that the keys are derived from a larger key. Nowhere in the reference indicates that the keys are derived from operation on data blocks. No matter how, each subblock of M, m_j (j = 0 ... 15) is processed, in parallel or serially (one by one), there is no disclosure in Den Boer that the keys are produced from datablocks. To the contrary, the embodiments of the present invention as claimed indicate that, at a preset conversion step, the value of subkeys is different in encrypting different data

supported by the original documents of the specification. A person of ordinary skill in the art is clear that the terms "dual-locus operation" and "two-place operation" within the scope of the submitted specification are equivalent and replacement of the term "dual-locus operation" with the term "two-place operation" does not alter the essence of the specification and of the claims. Thus, no new matter was introduced in the Applicant's response to the previous Official Action.

Therefore, the rejection under 35 U.S.C. § 112, first paragraph has been overcome. Accordingly, withdrawal of the rejections under 35 U.S.C. § 112, first paragraph, is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 102:

Claim 1 has been rejected under 35 U.S.C. § 102 (e) as allegedly being anticipated by Den Boer et al. (US 6,298,136), hereinafter Den Boer.

Applicant traverses the rejection and respectfully submits that the present-claimed invention is not anticipated by the cited reference. The embodiment of the present invention as defined in Claim 1 is different from the disclosure in Den Boer. The Examiner indicates that Den Boer discloses the conversion of data subblocks which are then used to convert subkeys (col. 4, lines 35 – 56). Applicant respectfully submits that the Examiner's understanding of the Den Boer reference is incorrect. Detailed study of the specification of Den Boer as a whole and its description at lines 35-65, column 4 has shown that the Examiner misunderstood its disclosure. The specification of Den Boer, at lines 35-65, column 4, contains use of confusing terminologies, which we believe has misled the Examiner. At lines 63-65 of the column 4, Den Boer discloses that "[T]o obtain the second K2, the cryptographic apparatus 400 comprises third input block 450". The Examiner makes the conclusion that Den Boer discloses converting a subkey by depending on the data block. However, this is incorrect. The description at lines 35-65, column 4 must be understood together with Fig.4 of Den Boer. In fact, what is meant by the term "third input block 450" is a third input unit for receiving subkey K2 and feeding

blocks. This is ensured by the fact that the subkeys are converted using the operation that depends upon subblocks of the data block being converted.

Therefore, the newly presented claim is not anticipated by Den Boer and the rejection under 35 U.S.C. § 102 (e) has been overcome. Accordingly, withdrawal of the rejection under 35 U.S.C. § 102 (e) is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 103:

Claims 2 – 4 have been rejected under 35 U.S.C. § 103 as allegedly being unpatentable over by Den Boer, in view of Coppersmith et al. (US 6,192,129), hereinafter Coppersmith.

Applicant traverses the rejection and respectfully submits that the embodiments of present-claimed invention are not obvious over Den Boer, in view of Coppersmith. As stated above, Den Boer does not disclose the invention as amended. Similarly, Coppersmith also fails to teach or suggest the embodiments of the present invention as defined in Claims 2 – 4. In Coppersmith, round subkeys are generated according to a determined law. Therefore, during the encryption of various data blocks, the value of subkeys remains unchanged over a preset conversion step of some preset round in the encryption methods described in Coppersmith. In addition, as admitted by the Examiner, Den Boer does not expressly disclose either an operation of permuting subkey bits or a substitute operation performed on a subkey as being the conversion operation step. Therefore, there is no motivation to combine Den Boer and Coppersmith. Even if they are combined, Den Boer and Coppersmith will not render the present claimed invention obvious. One of ordinary skill in the art would not discern the present invention as claimed at the time of its invention.

Therefore, the newly presented claims are not anticipated by Den Boer and Coppersmith and the rejection under 35 U.S.C. § 103 has been overcome. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103 is respectfully requested.

Having overcome all outstanding grounds of rejection, the application is now in condition for allowance, and prompt action toward that end is respectfully solicited.

Respectfully submitted,

JACOBSON HOLMAN PLLC

Date: February 9, 2005
(202) 638-6666
400 Seventh Street, N.W.
Washington, D.C. 20004
Atty. Dkt. No.: P65855US0

By _____
John C. Holman
Registration No. 22,769